Tjenestebeskrivelse

IPVPN

Versjon 7.5

13.01.2023

GlobalConnect

Table of contents

GlobalConnect

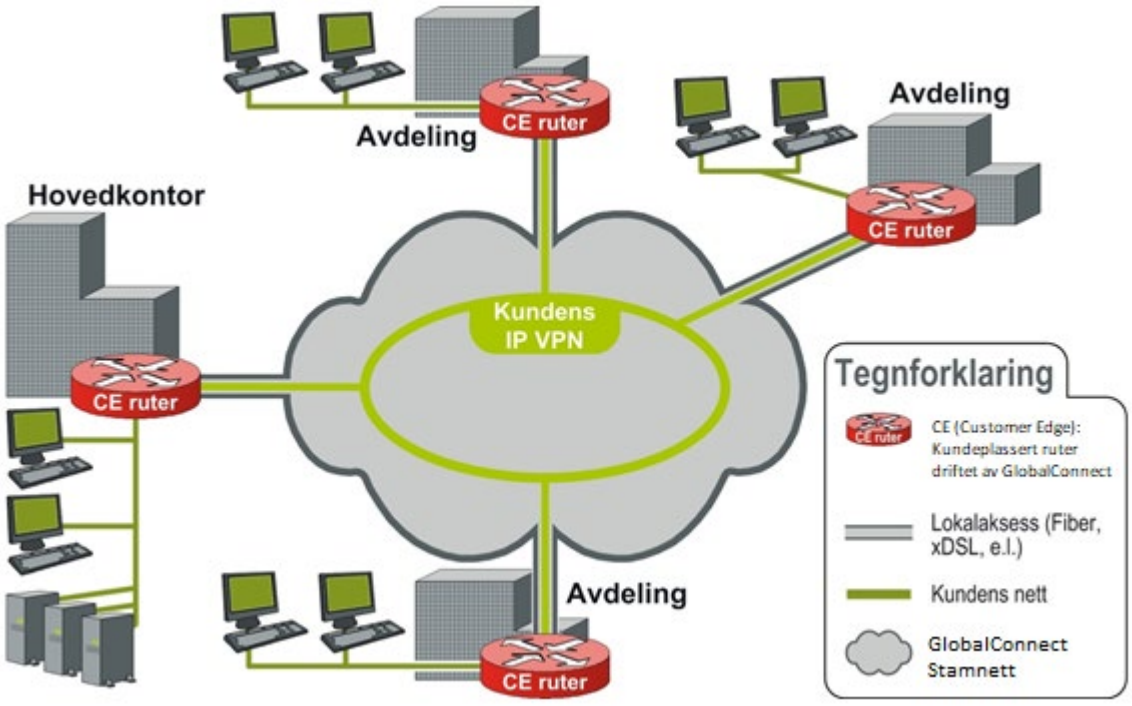
1 IPVPN

1.1 Introduksjon

IPVPN er en fleksibel datakommunikasjonstjeneste tilpasset det profesjonelle markedet i Norge med behov for et fremtidstrettet "Wide Area Network" (WAN). IPVPN realiseres over GlobalConnects landsdekkende MPLS-baserte kjernenett i Norge. GlobalConnect har i tillegg eget nett i Sverige og Danmark. Basert på dette kan nasjonale så vel som skandinaviske IPVPN/MPLS-baserte løsninger leveres. I tillegg gjør et samarbeid med utenlandske operatører det mulig å levere IPVPN globalt, der det er nødvendig.

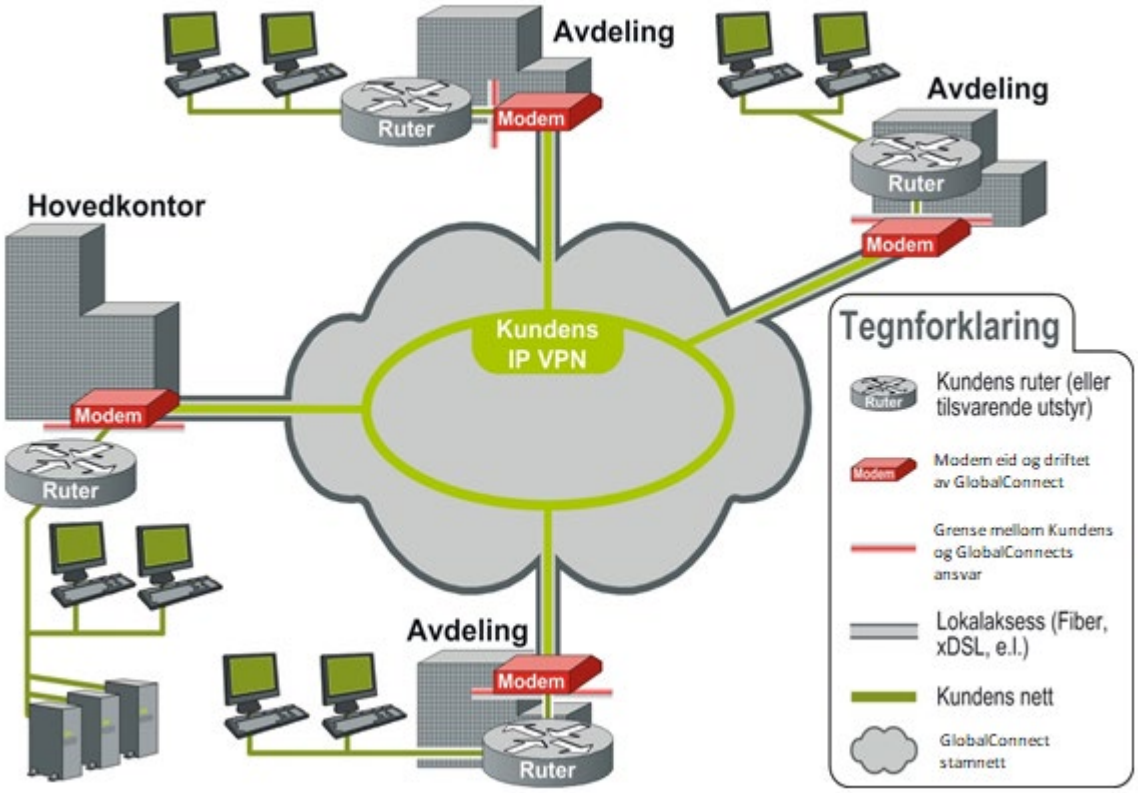
IPVPN leveres i to ulike varianter:

- **IPVPN Managed** er en driftet ende-til-ende tjeneste der GlobalConnect står for eierskap og drift av CE-ruter (Customer Edge) eller switch på kundelokasjonen. GlobalConnect er ansvarlig for løsningen ende-til-ende og overvåker tilgjengelighet og kvalitet helt frem til CE- ruters/switch' LAN-grensesnitt hos kunden. Løsningen passer for kunder som vil overlate hele WAN-driften til sin leverandør.



Figur 1-1: Prinsippskisse for en tenkt løsning med IPVPN Managed

- **IPVPN Unmanaged** er en driftet tjeneste der GlobalConnect er ansvarlig for løsningen frem til og med aksessmodemet. Løsningen passer for partnere som ønsker å videreselge IPVPN, eller for kunder som ønsker å eie, implementere og drifte CE-ruteren/switchen selv.



Figur 1-2: Prinsippskisse for en tenkt løsning med IPVPN Unmanaged

1.2 Funksjonalitet og kundefordeler med IPVPN Managed

- **Trafikkprioritering** sikrer trafikkflyt med prioritering av kritisk trafikk gjennom ulike **trafikklasser** med riktig **Tjenestekvalitet (Quality of Service, QoS)**
- **Alle-til-alle topologi (fully meshed)** der alle lokasjoner kan kommunisere direkte seg imellom eller mot nettsentriske tjenester hos GlobalConnect
- **Stjernetopologi (punkt-til-multipunkt)** for eksempel mot kundens hovedkontor eller datasenter
- **Ulike aksessformer;** Fiber, SHDSL, SHDSL.Bis, VDSL2, ADSL2+, Radio, Ethernet og Mobil PrimærAksess for best mulig tilpassing til kundens behov
- **Redundans** i form av linjeredundans og 4G backup
- **Diversitet** for enda bedre tilgjengelighet
- **MultiVPN** kan etableres for avdelingsnett, ekstranett eller lignende, og termineres som VLAN eller på separate porter på CE-ruteren
- **Nasjonal dekning** med mulighet for utvidet tilknytning av globale lokasjoner
- **Fleksible tjeneste** tilrettelagt for enkel opp/ned gradering av kapasitet samt legge til nye og fjerne eksisterende lokasjoner
- **Aktiv varsling** av kunden i feilsituasjoner der kunden ønsker dette
- **Trafikkstatistikk** tilgjengelig via web grensesnitt. Her har man tilgang til oppdaterte og historiske data for utnyttelse av båndbredde per lokasjon
- **Tilleggstjenester** for internettaksess, redundans, backup, MultiVPN, QoS, sikkerhet, Servicetid, Servicegaranti, betalingsaksesstjenester og mobile brukere
- **Tilgang til kvalifisert supportpersonell og feilmelding 24/7/365**, basert på valgt dekningsperiode
- **Service Level Agreement** som tilpasses hver kundelokasjons behov iht. servicegaranti og kostoptimalisering og krav til tilgjengelighet.

1.3 Funksjonsforskjeller mellom IPVPN Managed og IPVPN Unmanaged

Tabell 1-1 under gir en oversikt over funksjonsforskjeller mellom tjenestene IPVPN Managed og IPVPN Unmanaged.

FUNKSJONALITET	IPVPN MANAGED	IPVPN UNMANAGED
Alle-til-Alle (fully meshed) topologi	√	√
Stjernenett (punkt-til multipunkt)	√	Nei
MultiVPN	√	√
Trafikk prioritering/QoS	√	√
IPVPN o/Internett (IPsec)	√	Nei
Linjeredundans	√	Nei
Mobil Backup	√	Nei
Diversitet	√	Nei
Kryptering	√	Nei
Internet BreakOut	√	Nei
Service Level Agreement	√	√
VPNView 2.0	√	Nei
Aktiv varsling	√	Nei
SNMP read	√	Nei
Dekning	Globalt	Skandinavia

Tabell 1-1: Funksjonalitetsstøtte IPVPN Managed vs. IPVPN Unmanaged.

2 Teknisk funksjonalitet

2.1 Skalerbarhet

Med IPVPN kan kunden enkelt legge til nye lokasjoner i sin WAN-løsning, flytte eksisterende lokasjoner eller legge ned lokasjoner, om dette skulle være aktuelt. Kunden kan lett endre funksjonalitet på en eller flere lokasjoner. Endringer kan for eksempel omfatte IP-adresser eller funksjonalitet som QoS, redundans eller flere VPN i etterkant, der man ikke har installert dette fra dag en.

2.2 Aksessmetode og kapasitet

I utgangspunktet leveres aksessen fra kundelokasjon til GlobalConnects kjernenett (User Provider Edge UPE-ruter) på GlobalConnects egeneide infrastruktur. Om dette ikke er mulig, benyttes aksesser fra tredjepart operatør. IPVPN støtter i prinsippet alle aksessteknologier, deriblant fiber, Ethernet, digitale leide linjer, SHDSL,.Bis, VDSL og ADSL2+. Det kan finnes avvik i mulige aksessteknologier og kapasiteter som tilbys utenfor Norge.

Tabell 2-1 nedenfor spesifiserer aksessmetoder og kapasitet som leveres for IPVPN Managed.

AKSESSTEKNOLOGI	DSL LEVERANDØR	KAPASITET
Fiber og Ethernet	GlobalConnect egeneid	2 Mbps - 10 Gbps
Fiber og Ethernet	Alternativ leverandør	10 Mbps - 10 Gbps
SHDSL (oa)	GlobalConnect egeneid	1 – 20 Mbps
SHDSL (ws)	Alternativ infrastruktur	1 – 8 Mbps
VDSL (oa)	GlobalConnect egeneid	20 – 60 Mbps
VDSL (ws)	Alternativ leverandør	20 – 60 Mbps
ADSL (oa)	GlobalConnect egeneid	1 – 20 Mbps
ADSL (ws)	Alternativ leverandør	1 – 20 Mbps
Leid Linje*	Alternativ infrastruktur	2 – 8 Mbps
Mobil PrimærAksess(ICE)	Alternativ infrastruktur	8-300 GB
Utenfor Norge	Alternativ leverandør	per forespørsel

Tabell 2-1: Tilgjengelige aksessmetoder/kapasitet ***Kun på forespørsel.***

For detaljert informasjon om alternative hastigheter, se veiledende prisliste for IPVPN. Den aksess-metode/kapasitet som bestilles per lokasjon av kunde, er det som vil leveres dersom ønsket aksessform/kapasitet er tilgjengelig for lokasjonen.

2.2.1 ADSL og VDSL – Delt aksess

Benevnelsen delt aksess benyttes når kunden bruker den IPVPN-aksessen (ADSL/VDSL-basert) som ønskes benyttet for IPVPN til telefoni. Kostnaden for kobberleie deles i slike tilfeller mellom telefonitjenesten og IPVPN-tjenesten. Dersom kunden ikke har telefon på den aktuelle lokasjonen, eller kunden ønsker å få levert IPVPN-tjenesten på et dedikert kobberpar, kan IPVPN-aksessen tilbys uten telefoni dersom det er tilgjengelig trådpar.

2.2.2 IPVPN 4G Primær

IPVPN 4G Primær kobler lokasjonen til GlobalConnect sitt kjernenett med et mobil abonnement og et rutermodem. Kunden kan velge mellom flere typer abonnement, basert på ønsket GByte størrelse. Når forbruket overstiger bestilt volum, vil abonnementet automatisk justeres ned til 64Kbps. Det er mulig å oppgradere abonnementet når som helst i avtaleperioden, maks grense er 300GB.

Løsning mellom mobiloperatør og GlobalConnect sitt kjernenett er designet med et "carrier-grade" nivå. Det betyr redundans på lag 3 og diversitet på fysisk nivå.

Lokasjoner med IPVPN 4G Primær kan leveres med følgende datapakker pr måned:

PRODUKT*	DATAPAKKE
IPVPN 4G Primær ICE 8	8 GB
IPVPN 4G Primær ICE 18	18 GB
IPVPN 4G Primær ICE 35	35 GB
IPVPN 4G Primær ICE 50	50 GB
IPVPN 4G Primær ICE 100	100 GB
IPVPN 4G Primær ICE 300	300 GB

**Tjenesten er kun tilgjengelig i Norge. IPVPN Mobil PrimærAksess kvalifiserer til Servicegaranti 1.*

2.2.3 Grensesnitt

IPVPN Managed leveres med ruteren/switchens LAN-interface som grensesnitt, alternativer er: Fast Ethernet (FE) , Gigabit Ethernet (1GE) eller 10 Gigabit Ethernet(10GE)

2.3 Customer Edge ruter/switch

Som del av IPVPN Managed leveres en ruter eller switch, Customer Edge (CE) ruter/switch.

I utgangspunktet vil GlobalConnect designe kundens IPVPN-løsning med en passende ruter, eller i visse tilfeller en switch. CE-ruteren/switchen vil være tilpasset den kapasiteten og funksjonaliteten kunden ønsker per kundelokasjon.

Basert på den ruter- eller switch-modellen som benyttes, vil det kunne være begrensninger i den funksjonalitet som kan velges av kunden. Det vil også ev. kunne være begrensninger i hvilke funksjonalitet som kan legges til senere, uten å måtte bytte CE-utstyr.

2.4 Grensesnitt for ansvar

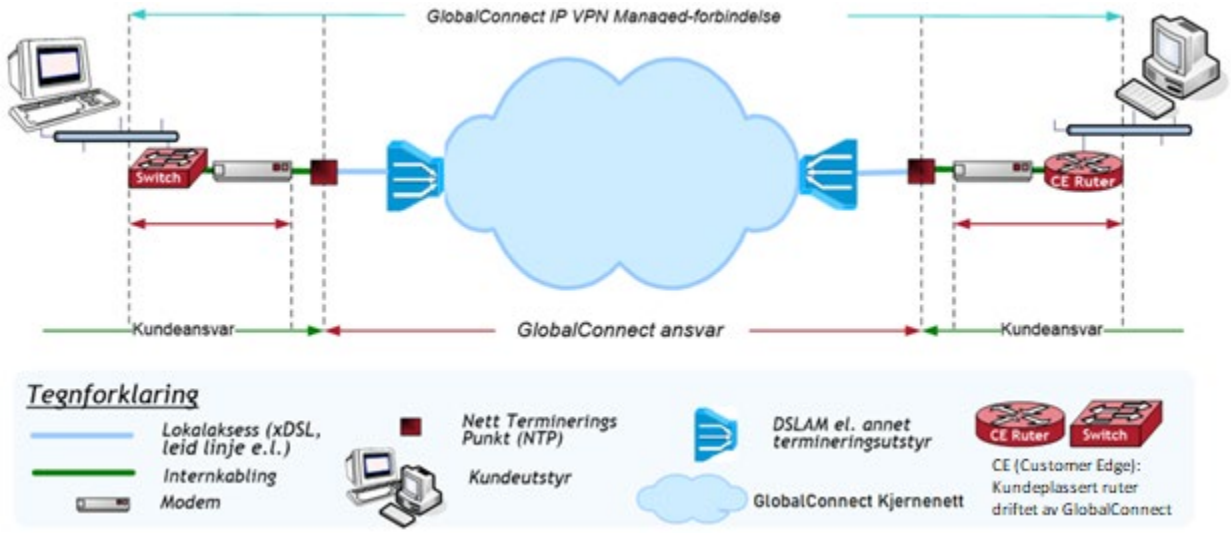
IPVPN Managed leveres med en CE-ruter/switch ved hver lokasjon eid og driftet av GlobalConnect.

Grensesnitt mellom kunden og GlobalConnect er CE-ruterens LAN-grensesnitt. GlobalConnect er ansvarlig for leveranse og drift av løsningen inklusive kapasitet i kjernenettet, lokalaksess med modem/konverter og CE-ruter/switch. Kunden er ansvarlig for lokalnettet og internkabling ved hver lokasjon, samt installasjon av modem og CE-ruter/switch. Montør kan bestilles for installasjon av modem og CE-ruter/switch hvis kunde ønsker dette.

Internkabling hos kunden er ikke inkludert i tjenesten IPVPN, og eventuelle kostnader relatert til feilsituasjoner/installasjon på internkabling fra netterminering spunktet (NTP) til modemet må dekkes av kunden.

Der aksessleverandør ikke eier internkabling, vil lokalaksessen leveres til NTP etter ”grunnmurs-prinsippet”. Bedriftsinternt nett fra NTP til montert RJ45-kontakt (eller annen) for tilkobling av aksessutstyr, er også kundens ansvar, det samme gjelder kostnader ved eventuell ny kabling og feilretting i bedriftsinternt nett.

GlobalConnect har driftsansvar for tjenesten jf. pilen benevnt ” IPVPN Managed-forbindelse” på Figur 2-1 under.



Figur 2-1: Oversikt over ansvarsområder og demarkasjonspunkt for IPVPN Managed.

Det er en forutsetning at termineringspunktet for lokalaksessen er plassert i umiddelbar nærhet av kundens LAN-tilkobling. Dette løses normalt ved internkabling som utføres av montørfirmaet som leverer aksessforbindelsen. Kunden er selv ansvarlig for bestilling og kostnader relatert til dette.

Som tilleggstjeneste kan Kunden få tilgang til SNMP leseaksess til CE-ruterne/switch. Med dette kan kunden i tillegg til GlobalConnect sin overvåkning, også benytte egne management-systemer mot løsningen.

Øvrig tilgang, som telnet og ”SNMP write aksess”, til CE-ruterne/switchene vil ikke bli gitt til kunden. Dette er blant annet for å unngå tvil om ansvar ved eventuelle feil som måtte oppstå i CE-ruterne/switchene og av sikkerhetsmessige årsaker.

2.5 Tekniske vilkår

Kvalitet i Leverandørens MPLS nett er bestemt av kriteriene angitt i dette kapittel. Aksessforbindelse som Leverandøren leier av andre leverandører mellom stamnett og Kundens lokaler, kan avvike fra disse kriterier.

2.5.1 Overføringskvalitet

Verdiene er gjennomsnittsverdier i normalsituasjonen, målt over en måned fra CE til CE. Kvalitets-parameterne for forsinkelse, pakketap og jitter gjelder ikke når aksesslinjene når metningspunkt over 75% utnyttelse av kapasitet, selv for korte tidsintervaller.

Trafikk profil	RT Voice	RT Video	Business	LAN	Bulk	Standard
DSCP value	46/EF	34/AF41	26/AF31	18/AF21	10/AF11	0/BE
Max packetloss	0,01%	0,05%	0,05%	0,1%	0,1%	0,1%
Max RTD<1200km	20ms	30ms	30ms	30ms	40ms	40ms
Max RTD >1200km	40ms	50ms	50ms	50ms	55ms	55ms
Max jitter*	5ms	10ms	10ms	10ms	15ms	15ms

**Aksesser med A/VDSL teknologi inngår ikke i garantiene for overføringskvalitet for Jitter og Pakketap*

Tabell 3-4 – Overføringskvalitet.

Måling av pakketap: Den prosentdel av data som sendes i nettet men som ikke når frem til destinasjonen. Data innsamles fra utvalgte rutere i sentrale terminaler med et intervall på fem minutter. Månedlige statistikker på forsinkelse og pakkeleveranser utregnes på basis av et gjennomsnitt av alle prøver fra foregående måned. Pakketap beregnes med nedenstående formel:

$$Pakketap(\%) = \frac{antall\ pakker\ tapt}{antall\ pakker\ sent} * 100$$

Måling av forsinkelse: Forsinkelse er den tiden det tar å sende en datapakke fra avsender til mottaker (enveis forsinkelse). GlobalConnect måler forsinkelse i form av Round Trip Delay (RTD) som tilsvarer forsinkelse fra avsender til mottaker og tilbake til avsender.

Måling av variabel forsinkelse (jitter): Variasjoner i forsinkelse defineres som jitter.

2.5.2 Nettverksprotokoller

IPVPN er beregnet på transport av IP, per i dag IPv4. Ruting mellom lokasjonene skjer basert på IP. Det forutsettes at kunden benytter forskjellig IP-subnett ved hver lokasjon. Kunden kan både benytte uoffisielle IP-adresser (RFC 1918) og offisielle IP-adresser i nettet.

2.5.3 Pakkestørrelse

MTU (Maximum Transmission Unit) spesifiserer hvor mange bytes som kan overføres i en IP-pakke. MTU pakkestørrelse for IPVPN er 1500 Bytes. Dette er samme pakkestørrelse som i de fleste Ethernet-baserte LAN og som også benyttes som standard i blant annet Microsoft Windows. Pakkestørrelsen kan differensiere noe ved bruk av Mobil Backup og Kryptering(AES). Tjenesten tilbyr MTU 1600 som opsjon for større MTU.

2.5.4 DHCP (Dynamisk IP-tildeling)

Den enkelte CE-ruter kan settes opp med DHCP forwarding (også kjent som ”IP helper adresse”) for sentral DHCP-server hos kunden. GlobalConnect setter ikke opp DHCP-server lokalt på den enkelte CE-ruteren, da vi med dette måtte involveres i drift av kundens LAN.

2.6 Nettverkstopologi

IPVPN inkluderer standard ‘Fully meshed* VPN topologi. Som en opsjon kan løsningen settes opp som et stjernenett (Hub&Spoke / punkt-til-multipunkt).

Ved valg av HUB&Spoke kan GlobalConnect ut fra kundens behov tilpasse i hvilken grad indirekte kommunikasjon mellom lokasjonene skal være tillatt.

GlobalConnect tilbyr en versjon av Hub&Spoke, der trafikken på HUB siten vil separeres logisk på inngående- og utgående-trafikk. Tjenesten overleveres mot kundens LAN, enten på en fysisk port, separert på VLAN for inngående og utgående trafikk, eller på to fysiske porter.

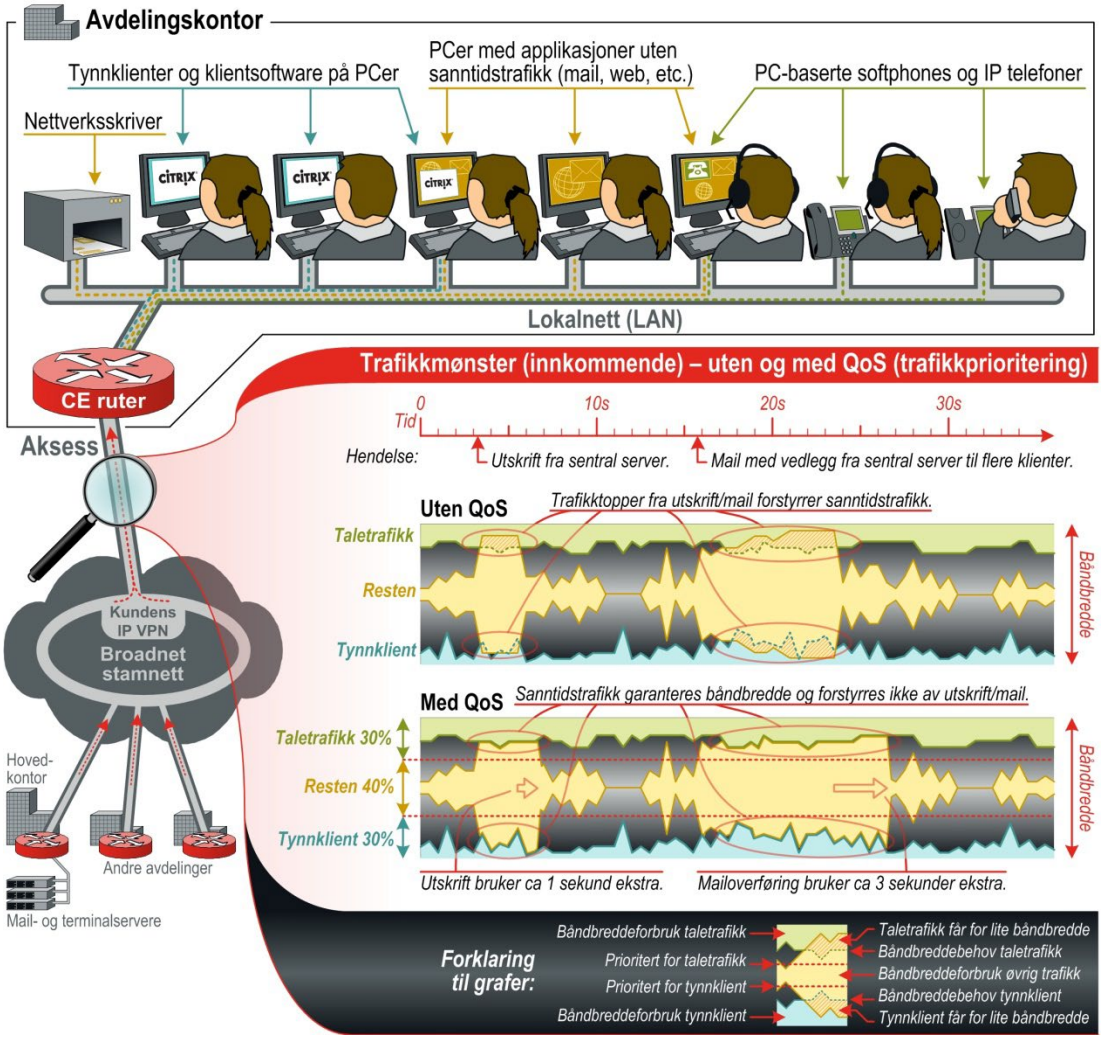
3 Quality of Service (QoS)

3.1 Tjenestekvalitet

Med tjenestekvalitet, menes i denne sammenheng den kvaliteten som er definert for IPVPN Managed og/eller brukerens kvalitetsopplevelse med hensyn til kvalitetsparameterne jitter (variasjon i forsinkelse), forsinkelse, pakketap og tilgjengelig båndbredde. Forskjellige trafikktyper/applikasjoner har ulike krav til tjenestekvalitet og er av ulik forretningskritisk viktighet for kunden. Dette løses ved å prioritere trafikken i ulike trafikklasser med ulike kvalitetsnivåer.

3.2 Trafikkflyt ikke trafikkaos

I en WAN-løsning vil kunden kjøre mange ulike applikasjoner med ulik viktighet for selskapets forretning og med ulike kvalitetsbehov. Det er viktig at alle applikasjonene har riktig arbeidsforhold for å fungere tilfredsstillende for brukerne. Figur 3-1 under viser en prinsippskisse der en bedrifts brukerne samtidig forsøker å benytte en rekke ulike applikasjoner som IP-telefoni, ERP-systemer, videokonferanse, browsing på Internett og sending av e-post.



Figur 3-1: WAN-løsning der brukere samtidig forsøker å kjøre en rekke ulike applikasjoner.

Trafikken begynner å gå tregt og applikasjonene fungerer ikke som de skal, til slutt er det så og si umulig å benytte både IP-telefoni, videokonferanse eller ordresystem.

3.3 Trafikkflyt

Løsningen vil her være å innføre QoS/Trafikkprioritering. Kundens ulike applikasjoner fordeles og tilpasses ulike trafikklasser med riktig kvalitet. Slik sikres god flyt for all type trafikk.

Prioritering av trafikk gjennom å benytte ulike trafikklasser med ulik kvalitet, er ofte en bedre løsning enn kun å øke på med mer båndbredde, da arbeidsforholdene til applikasjonene også sikres. Det er imidlertid viktig å merke seg at antall samtidige videokonferanser og/eller telefonsamtaler må avstemmes med tilgjengelig båndbredde.

3.4 Trafikkprioritering og trafikklasser

For å prioritere kundens ulike applikasjoner må det være mulig å skille disse applikasjonene i forskjellige trafikklasser. GlobalConnect tilbyr ulike trafikklasser tilpasset ulike applikasjoners karakteristikk og identifiserte (klassifiserte) applikasjoner plasseres i ønsket/riktig klasse.

Hver trafikklasse leveres med et sett av kvalitetsparametere med gitte verdier;

- Jitter – variasjon i forsinkelse
- RTD (Round Trip Delay) – forsinkelse
- Pakketap

IP-telefoni er for eksempel avhengig av lavt pakketap og liten variasjon i forsinkelse (jitter) for å fungere tilfredsstillende. Sanntids video har de samme kravene til begrenset jitter og pakketap, men har et helt annet trafikkmønster med variable pakkestørrelser og ekstremt ulik pakke rate, og bør derfor i en annen trafikklasse enn IP-telefoni. Terminaltrafikk (for eksempel Citrix) berøres spesielt av høy forsinkelsen gjennom nettet.

Disse applikasjonseksemplene er således avhengig av kontinuerlig båndbredde og riktig kvalitet, og kan påvirkes negativt dersom tilgang til båndbredde i perioder begrenses av annen trafikk og/eller kvaliteten i nettet forringes. Dette kan motvirkes ved at kritisk trafikk identifiseres og gis prioritet foran mindre kritisk trafikk som for eksempel e-post replikering og webtrafikk, og at applikasjonene sendes i trafikklasser med et kvalitetsnivå tilpasset den enkelte applikasjons karakteristikk.

IPVPN er designet for å gjenkjenne og prioritere 6 trafikklasser, og Tabell 3-1 nedenfor viser hvilke klasser som er definert og eksempler på type applikasjoner som kan passe i hver klasse.

Trafikklasser	Applikasjonstyper	Applikasjonseksempler
Voice	For typiske sanntidsapplikasjoner som er vare for variasjon i forsinkelse, forsinkelse og pakketap	Telefoni
Video		Videokonferanse, sanntid
Business	Interaktiv trafikk som ERP-applikasjoner og andre applikasjoner som er vare for forsinkelse og pakketap	IFS, SAP, Citrix, Movex
LAN	Interaktive applikasjoner med små overføringsmengder, eller trafikk som ønskes prioritert etter Business – mindre forretningskritisk	Betalingstransaksjoner, måleadata
Bulk traffic	”Store dataoverføringer” som ikke er sensitive til forsinkelse eller pakketap	Backup/restore og replikering av store datamengder, video content distribusjon
Standard	Robuste- og ikke forretningskritiske applikasjoner	Internett-browsing (ftp), e-post, backup, replikering

Tabell 3-1: Definerte trafikklasser og eksempler på applikasjonstyper og/eller applikasjoner.

Trafikklassene kan deles i to grupper:

- Voice- og Video-klassene er av typen “sann tid” (RealTime)
- De resterende klassene omtales som “Data-klasser”

All trafikk som ikke er spesielt klassifisert, vil legges i Dataklassen “Standard”. Dette vil også gjelde for kunder som ikke bestiller Trafikkprioriterings-produktet.

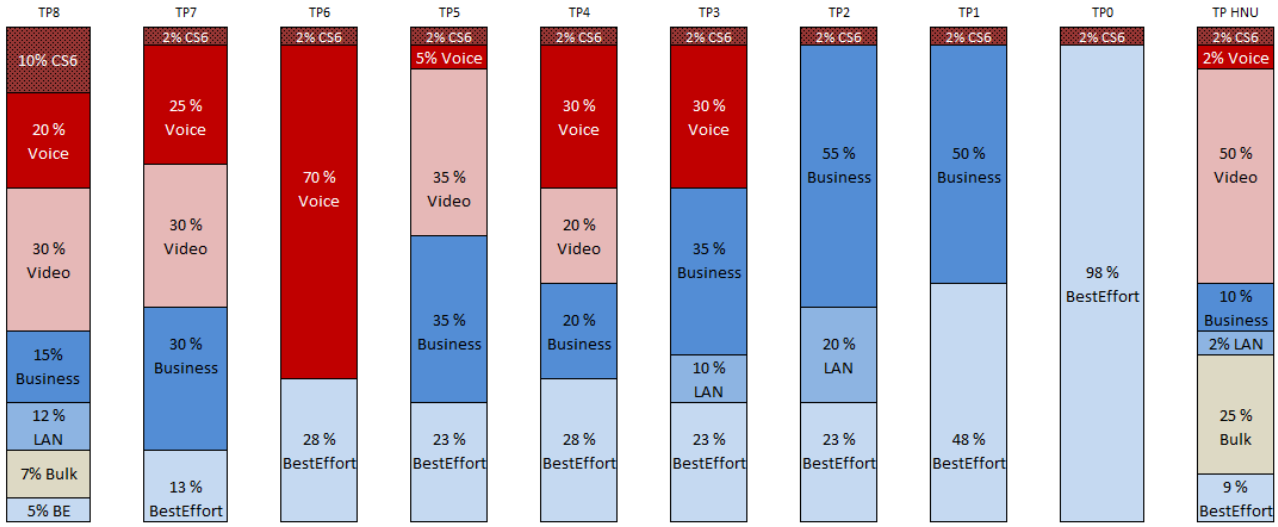
3.5 Trafikkprofiler

Et sett trafikkprofiler er designet basert på de trafikklassene som er definert for prioritering av ulike applikasjoner. Profilene er satt sammen av de ulike trafikklassene basert på “best practise” og GlobalConnects erfaring.

Kunden velger den profilen som passer best per lokasjon ift. hvilke applikasjoner som skal benyttes i løsningen, basert på applikasjonskarakteristikk og forretningsmessige hensyn. Kunden må selv avgjøre hvilke applikasjoner som ønskes prioritert og hvilke trafikklasser som skal benyttes. Det er imidlertid viktig at løsningen designes med tanke på hvilke lokasjoner som skal kommunisere med hvilke, slik at prioriteringsmekanismene kan utnyttes fullt ut. Det er for eksempel viktig at en profil med RealTime Voice velges på alle lokasjoner som skal kjøre IP-telefoni selv om det er mulig å benytte ulike profiler i en løsning. Det er i utgangspunktet de samme profilene som benyttes uansett aksessform. Det er imidlertid slik at for xDSL-aksesser så “shapes” kapasiteten ned til nærmeste hele Mbps.

3.5.1 Standard profiler

Se Figur 3-2 under for en visualisering av tilgjengelige standard trafikkprofiler. Profilene er designet for å kunne prioritere ulike trafikklasser samtidig, avhengig av valgt profil.



Figur 3-2: Definerte standard trafikkprofiler(TP).

CS6 klassen, Class Selector 6 med DSCP verdi EXP 6: Leverandøren kan benytte inntil 2% av den totale kapasiteten til signalering/driftsrelatert trafikk. Når denne klassen ikke benyttes, tilkommer denne kapasiteten BestEffort klassen. TP8 er spesialtilpasset for kunder som har utvidet behov for signalerings kapasitet og har således CS6 satt til 10%.

3.5.2 Trafikkprofiler ved bruk av partnere

Ved leveranse av IPVPN utenfor Norge benytter GlobalConnect seg av partnere for leveranse av IPVPN-aksesser for tilknytning til GlobalConnects nett. Det er nødvendig og hensyn-ta hvilke trafikkprioritering og QoS-nivå disse Leverandørene leverer. GlobalConnect har imidlertid tilstrebet å designe profiler som er best mulig tilpasset de profilene som er definert for leveranse i Norge.

3.5.3 Design av løsning med trafikkprioritering

Design og implementering av en MPLS-basert WAN-løsning med trafikkprioritering krever dybdekompetanse både om hvordan tjenestekvalitet (QoS) og trafikkprioritering fungerer samt kunnskap om kundens nettløsning og applikasjoner.

En løsningsdesigner hos GlobalConnect vil derfor kunne bistå i denne prosessen som en del av IPVPN Managed-tjenesten. I samarbeid med kunden vil det identifiseres hvordan kundens spesifikke applikasjoner bør prioriteres for best å utnytte de enkelte trafikklassene og designe en optimal nettløsning basert på kundens krav og forretningsmessige behov.

3.5.4 Trafikklassenes funksjonalitet

3.5.4.1 Fleksibilitet

Selv om trafikkprioritering for IPVPN Managed er basert på forhåndsdefinerte profiler, er tjenesten basert på stor grad av fleksibilitet.

Kunden behøver ikke å benytte alle trafikklassene i en valgt profil. Dette gjør det mulig for kunden å tilpasse tjenesten til sine behov, og båndbredden per lokasjon vil utnyttes best mulig samtidig som det hensyn tas at applikasjonene skal fungere optimalt iht. angitt karakteristikk.

3.5.4.2 RealTime-klassene

Basert på karakteristikken til typiske sanntids-applikasjoner vil all trafikk i RealTime-klassene som kjører ut over det valgte profil er designet for bli kastet. Dette for å kunne sikre kvaliteten som er påkrevet for at disse typer applikasjoner skal fungere optimalt. Audio-delen for Video-klassen vil gå i Voice-klassen dersom denne trafikken merkes som voice. Enkelte videosystemer merker imidlertid voic-delen også slik at den vil gå i videoklassen. Ved behov for mer plass til sanntids-applikasjoner må tilgjengelig båndbredde for den spesifikke lokasjonen økes, eller maksimalt antall telefoni- og/eller videokanaler som kan settes opp samtidig fra/til Lokasjonen, må reduseres.

3.5.4.3 Dataklassene

Trafikk i Dataklassene kan benytte ledig kapasitet, også ut over det profilen er designet for.

Dersom det kjøres for mye trafikk i en Dataklasse kastes denne kun dersom de øvrige klassene kjører fullt ut det de er designet for. Dette for å sikre god trafikkflyt for all trafikk, samt å sikre riktig kvalitet for de applikasjonene som kjører.

Kvalitetsnivået for trafikk som kjører over en annen klasse enn det applikasjonen(e) er designet for, kan imidlertid ikke garanteres. Det kan derfor være behov for å øke tilgjengelig båndbredde for å få riktig effekt av trafikkprioriteringstjenesten.

3.5.4.4 Eksempel på hvordan trafikken vil flyte

Kunden velger Trafikkprofil 3, 30% RealTime Voice, 35% Business, 10% LAN (Transaction) og 25% Standard. Denne trafikkprofilen installeres på hovedkontoret, med en IPVPN-aksess på 20 Mbps, og så ledes total tilgjengelig båndbredde.

1. Kunden sender 30% Voice-, 10% LAN- og 25% Standard-trafikk. I tillegg sender kunden mer enn 35% Business-trafikk, eks. 50%. I dette tilfelle vil da 15% av Business-trafikken kastes. Trafikken i de øvrige klassene får sine tilmålte båndbredder og kvalitet. Kunden kjører i dette tilfellet for mye trafikk totalt og bør oppgradere sin IPVPN-aksess, altså øke tilgjengelig båndbredde, dersom dette er en normal situasjon.
2. Om kunden derimot ikke utnytter de øvrige trafikklassene fullt ut, vil det kunne se slik ut; kunden sender fortsatt 30 Voice, men ikke trafikk i LAN-klassen og kun 20% i Standard-klassen og kan dermed sende 50% Business-trafikk og fortsatt ikke overstige de tilgjengelige 20 Mbps. 30% som er den garanterte båndbredden, i tillegg til 15% som “lånes” fra de øvrige Dataklassene som er definert for Profil 3. Riktig kvalitetsnivå garanteres imidlertid kun for den trafikken som går innenfor

30%.

3. Kunden forsøker å sette opp flere samtidige telefonsamtaler enn det de 30% Voice-kapasitet som Profil 3 gir tilgang til, altså ønsker å kjøre Voice-trafikk over 30%. All Voice-trafikk som overstiger 30% (av 20 Mbps) blir kastet.

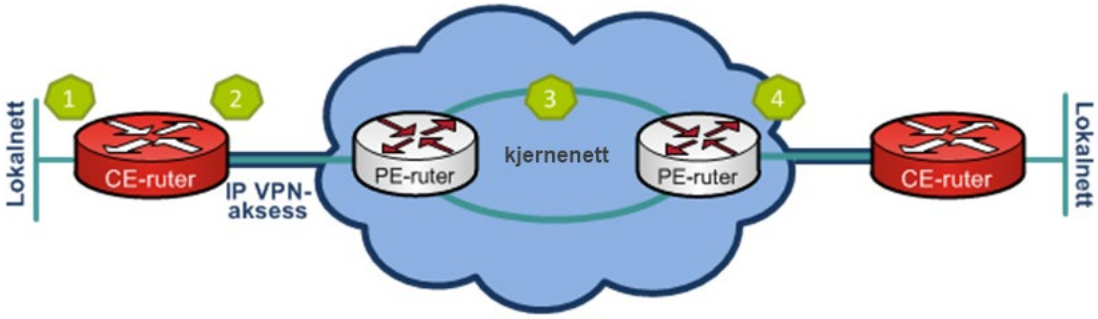
-

3.5.5 Implementering av trafikkprioritering

Trafikkprioritering implementeres over IPVPN-aksessen. Trafikken prioriteres både inn fra CE-ruteren (kundesiden) og ut fra PE-ruteren (nettsiden). Kundens applikasjoner legges inn i riktig trafikklasse og prioriteres og transporteres basert på de kvalitetsparametere som er definert for den gitte trafikklassen.

1. Trafikken klassifiseres på CE-ruterens LAN port (kundesiden)

2. Trafikken prioriteres på CE-ruterens WAN port og “shapes” iht. kapasiteten på IPVPN-aksessen (kundesiden)



3. Trafikken beholder informasjon om klassifisering og prioritering gjennom kjernenettet

4. Trafikken prioriteres ut fra PE-ruteren (nettsiden) og ”shapes” iht. kapasiteten på IPVPN-aksessen

3.5.6 Merking av trafikk

For å kunne sende ulike trafikktyper (applikasjoner) i riktig klasse må trafikken merkes. Applikasjonene vil enten bli merket i CE-ruteren av GlobalConnect, eller kunden vil merke trafikken sin selv – herunder også der merkingen ligge ferdig i applikasjonen.

Det er mulig å kombinere de to måtene å klassifisere trafikken på; GlobalConnect klassifisert- og Kunde klassifisert merking.

All trafikk som ikke er spesielt merket, vil legges i Dataklassen “Standard”.

GlobalConnect klassifisering av trafikk

Dersom GlobalConnect skal merke trafikken gjøres dette basert på hva kunden selv spesifiserer, og/eller på et ferdig definert oppsett basert på kjente porter, se 0 nedenfor. Det er trafikk i Businessklassen som merkes ved bruk av standardoppsettet.

Applikasjonene som kjøres i nettet, for eksempel IP-telefoni og ulike ERP-applikasjoner, identifiseres av GlobalConnect driftet CE-ruter ut fra de spesifikasjonene kunden gir.

Klassifiseringen av trafikken kan være basert på kjente porter, kundespesifikke TCP/UDP- porter, (sub-) interface eller source og/eller destinasjons IP-adresser. Det er også mulig for GlobalConnect å re-merke basert på kundens egen merking.

Kunde klassifisering av trafikk

Dersom kunden selv velger å merke trafikken må det gjøres iht. DSCP-verdiene som er spesifisert i Tabell 3-2 nedenfor. Applikasjonene legges i de ulike trafikklassene basert på denne identifiseringen.

Trafikklasser	DSCP-verdier	Betegnelse (DSCP PHB)	
Voice	46	EF	Expedited Forwarding
Video	34	AF41	Assured Forwarding
Business	26	AF31	Assured Forwarding
LAN (Transaction)	18	AF21	Assured Forwarding
Bulk traffic	10	AF11	Assured Forwarding
Standard	0	BE	Best Effort

Tabell 3-2: DSCP-verdier definert for de ulike trafikklassene.

Dersom CE-ruteren (driftet av GlobalConnect) håndterer identifiseringen, trenger ikke kunden forholde seg til disse DSCP-verdiene.

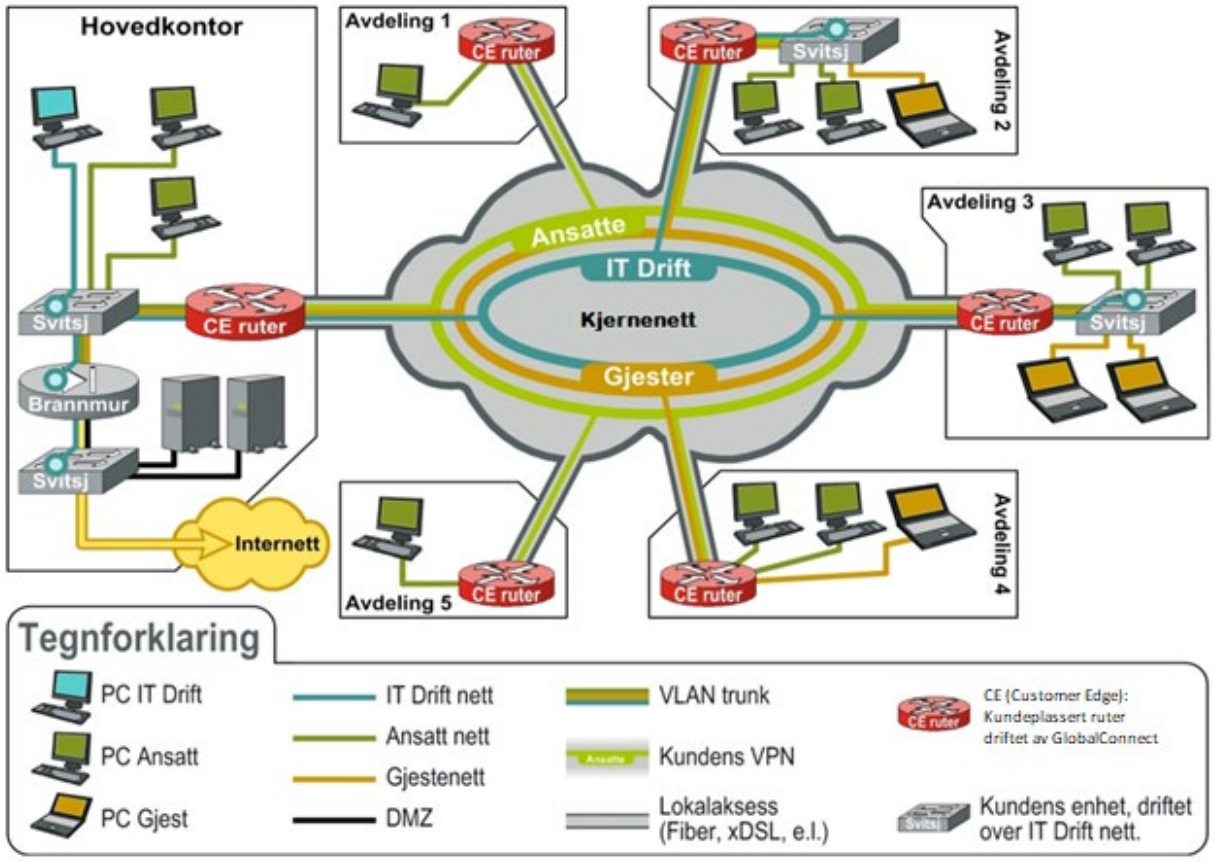
Da ADSL og VDSL har en asymmetrisk realisering, støtter ikke disse aksessformene QoS.

4 Tilleggstjenester

4.1 MultiVPN

En nettløsning basert på IPVPN Managed kan designes til å inneholde flere separate nett/VPN i parallell, MultiVPN. Enheter på hvert av de separate nettene kan kommunisere med hverandre over IPVPN-løsningen. Samtidig tillater ikke IPVPN Managed trafikk mellom ulike separate VPN.

Prinsippet kan enklest forklares med et eksempel:



Figur 3-1 Eksempel på bruk av IPVPN med MultiVPN.

Figur 3-1 ovenfor viser en tenkt løsning for en bedrift som både har PC-er benyttet av ansatte og PC-er benyttet av gjester. Etter som besøkende ikke skal ha tilgang til bedriftens interne systemer er det behov for separasjon av nettene. Da både ansatte og gjester skal ha tilgang til Internett og sentrale systemer som ligger på hovedkontoret må imidlertid begge de separate nettene transporteres mellom bedriftens avdelinger. I tillegg skal IT-driftspersonell på hovedkontoret kunne fjernadministrere switcher ved flere av bedriftens avdelingskontorer uten at bedriftens øvrige ansatte skal ha tilgang til disse.

Dette betyr at det er behov for transport av 3 nett parallelt, for henholdsvis IT-drift, ansatte og kunder. Hver CE-ruter har kun fysiske eller logiske LAN-interfaces for de nettene som er representert ved avdelingen der de er plassert. Avdeling 1 og 5 i eksemplet har kun PC-er for ansatte og ingen svitsjer som skal fjerndriftes. Dermed har de bare nettet for ansatte representert. Avdeling 2, 3 og 4 har PC-er både for gjester og ansatte, og har nett for både kunder og ansatte representert. Avdeling 2 og 3 har i tillegg

switcher som driftes fra IT-avdelingen sentralt, og har dermed IT-driftsnettet representert.

CE-rutere kan enten levere hvert separate VPN på separate fysiske grensesnitt eller på ett grensesnitt separert med VLAN mot en switch. I figur 3-7 er dette eksemplifisert med flere fysiske grensesnitt ved avdeling 4 og VLAN ved hovedkontoret samt avdeling 2 og 3. CE-ruterne og IPVPN-løsningen som helhet holder de separate nettene helt og holdent atskilt. Sikkerhet mot felles ressurser og Internett ivaretas av brannmurer på hovedkontoret som bedriften selv administrerer. Sikkerheten mellom de separate nettene er på denne måten helt og holdent under bedriftens kontroll.

4.1.1 MultiVPN og nettverkstopologi

IPVPN Managed kan leveres både som stjernenett og med alle-til-alle topologi, se kapittel 2.6 ovenfor.

Når MultiVPN nett leveres kan det finnes begrensninger i hvor mange av disse nettene som kan leveres som alle-til-alle (fully meshed) nett. Ev. begrensninger vil kunne føre til at kun ett VPN kan leveres som fully meshed, og de øvrige må implementeres som stjernenett. For stjernenettene er det opp til kunden, per VPN, om kommunikasjon mellom de enkelte lokasjonene skal være tillatt.

4.2 Redundans

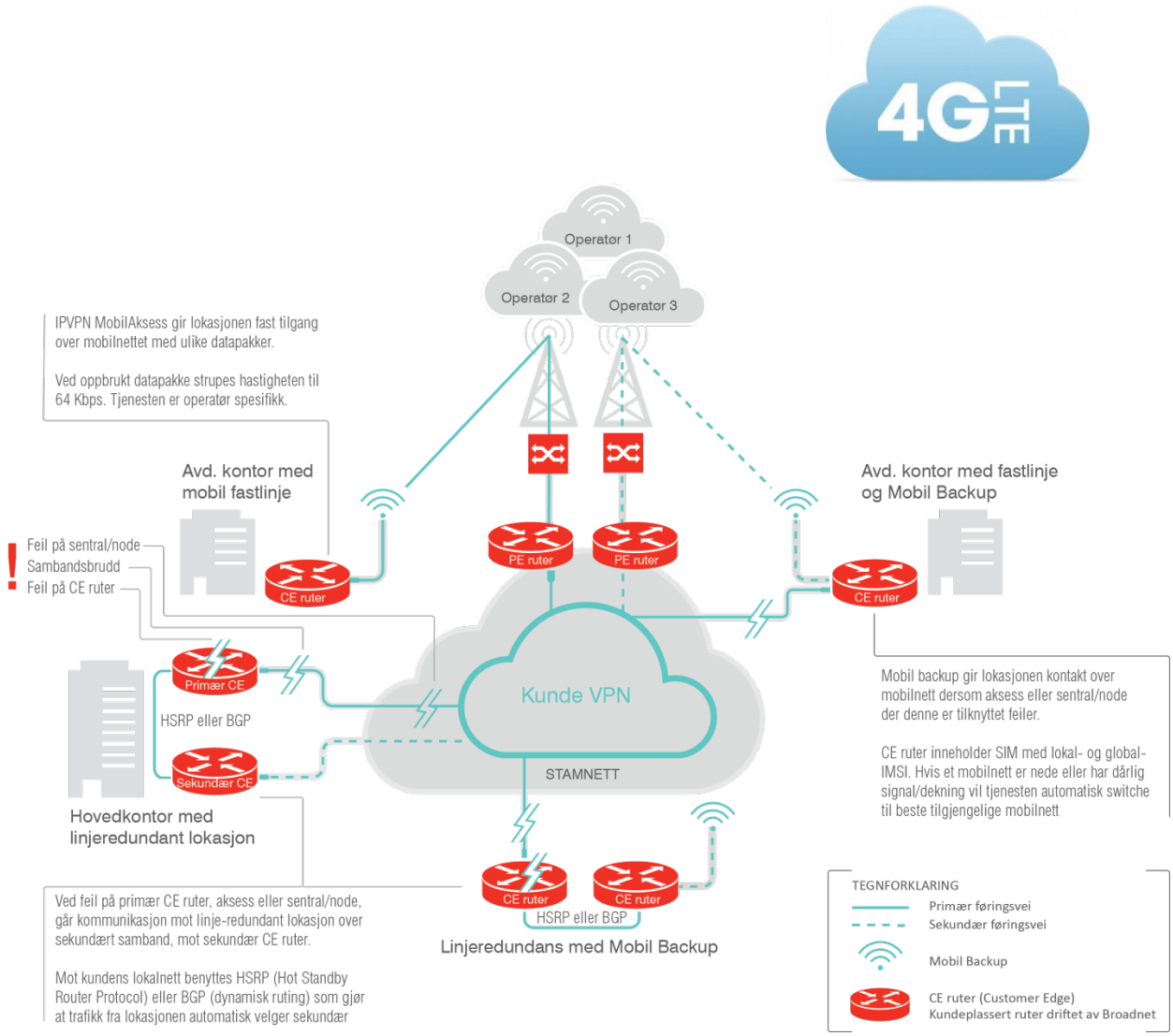
For kundelokasjoner med ekstra krav til oppetid, som for eksempel hovedkontoret eller et datasenter der applikasjonene er sentralisert, tilbys flere variasjoner for redundans. Avhengig av hvilken type redundans som velges, vil dette redusere risiko for nedetid. GlobalConnects redundante løsninger bygger på at sekundærforbindelsen kun er i bruk i feilsituasjoner.

Figur 4-2 under illustrerer de ulike grader av redundans som tilbys og hvordan disse kan kombineres i en og samme løsning. Følgende tjenestevarianter tilbys: IPVPN Linjeredundans, IPVPN Mobil Backup og Diversitet.

4.2.1 IPVPN Linjeredundans

For lokasjoner med spesielt høye krav til oppetid, som for eksempel datasenteret, er linjeredundans et godt alternativ. På kundelokasjonen installeres to CE-rutere med hver sin IPVPN aksess. Det kreves at primær- og sekundæraksessen leveres i uavhengige adskilte føringsveier eller er basert på 4G. Overgang fra primær til sekundær CE-ruter og aksess skjer automatisk ved bruk av en dynamisk ruting protokoll, f eks. HSRP (Hot Standby Routing Protocol). For løsninger med Linjeredundans med HSRP (eller andre dynamiske ruting protokoller på LAN siden av ruteren) så må kundens LAN kunne transportere protokollen(HSRP) mellom disse to CE-rutere.

IPVPN Linjeredundans kan også benyttes til å bygge redundans mot geografisk adskilte enheter, for eksempel primært og sekundært datasenter. Det kreves at kunden har en forbindelse mellom de to lokasjonene utenom WAN-et. Primæraksessen i en redundant løsning leveres som fiber, mens sekundæraksessen leveres som xDSL eller som fiber. Vær nøye med hvilken type Linjeredundans som benyttes, da de gir ulik Servicegaranti avhengig av hvilken teknisk realisering som benyttes. Kobber/xDSL vil ikke gi tilgang til Servicegaranti 3. Sekundær aksess kan også realiseres med Mobil Backup 4G, ref. figur Figur 4-2: IPVPN Managed-løsning med linjeredundans på sentral lokasjon og avdelingskontorer med hhv Mobil backup, Mobil PrimærAksess og Linjeredundans m/Mobil Backup. Det vil alltid kreves en evaluering av de faktiske forholdene for en lokasjon før IPVPN Linjeredundans kan tilbys.



Figur 4-2: IPVPN Managed-løsning med linjeredundans på sentral lokasjon og avdelingskontorer med hhv Mobil backup, Mobil PrimærAksess og Linjeredundans m/Mobil Backup.

Lokasjoner med IPVPN Linjeredundans vil kvalifisere til kvalitetsnivå 2 eller 3, avhengig av løsningsdesign. Enkeltstående feil vil i utgangspunktet ikke gi nedetid for en lokasjon med linjeredundans. For å oppnå kvalitetsnivå 3 forutsettes det at xDSL ikke benyttes på primær eller sekundær samband. Se for øvrig kapittel 5.3 Servicegaranti.

4.2.2 IPVPN 4G Backup

Med 4G Backup vil en lokasjon fortsatt ha kommunikasjonsmuligheter dersom en feil skulle oppstå med kjernenettet, modemet eller IPVPN aksessen. Dette skjer ved at CE-ruteren automatisk svitsjer over til mobil-nettet for fortsatt overføring av datatrafikk i en feilsituasjon. Overgangen til backup løsningen vil kunne ta 20-120 sekunder.

4G Backup installeres per kundelokasjon, som ønsker mulighet for backup. Dersom kunden har implementert flere VPN, må det spesifiseres hvilke VPNer det ønskes backup for.

GlobalConnect sin unike løsning er designet for best mulig tilgjengelighet og for å minimalisere utfordringer med mobildekning eller signalforhold. Som eneste leverandør i Norge tilbyr GlobalConnect en backupløsning som gir mulighet for roaming. Dette betyr at vår løsning vil velge den operatøren som har best dekning og signalforhold, og bytte hvis forholdene skulle endre seg. Vår primære operatør er Telia.

For å sikre at kundens mest kritiske trafikk/applikasjoner slipper igjennom i en backup situasjon, kan det settes opp aksesslister i CE-ruteren som styrer dette. Det defineres en aksessliste per VPN, og den må være den samme for alle lokasjoner med Mobil Backup for det gitte VPNet. 4G Backup tilbys primært i Norge, men inkluderer løsning for Skandinavia. Tjenesten inkluderer Mobil-abonnementet og trafikkost i en feilsituasjon. Imidlertid, dersom feil på en lokasjon, er GlobalConnect avhengig av at kunde responderer på henvendelser fra oss, slik at primær forbindelse kan rettes så raskt som mulig. For kunder som ikke responderer og det er stor sannsynlighet for overforbruk av data, vil GlobalConnect shape hastigheten ned til maks 1 Mbps etter et døgn, uten tilbakemelding fra kunde. Skulle dette medføre at det går mer enn 5GB trafikk over backup-løsningen i løpet av en måned, vil trafikk over 5GB bli fakturert kunde basert på kost +10%.

Hvor effektiv Mobil Backup-tjenesten er, vil være helt avhengig av distansen fra kundelokasjonen til base-stasjonen(e) og signal styrke/interferens. I tillegg er signalforhold på kundelokasjon avgjørende for dekningen. Utstyr kan ikke plasser på steder der dekningsforhold forringes. F eks skap, kjeller rom eller lignende, uten at antenne er plassert mest mulig hensiktsmessig for signalforholdene.

Lokasjoner med IPVPN 4G Backup kvalifiserer til Servicegaranti 2, basert på at lokasjonen har dekning i en feilsituasjon. Feilsituasjoner når 4G Backup er aktiv, behandles som unntatt tid i SLA refusjons kalkulasjon.

4.2.3 Kapasitet og stabilitet

GlobalConnect kan ikke garantere for den kapasiteten som kan oppnås på den mobile forbindelsen i en feilsituasjon, eller at det faktisk er dekning på lokasjonen i en feilsituasjon.

I salgsprosessen kan GlobalConnect teoretisk estimere signalforholdet på en adresse, men det er signalstyrken inne i bygget som avgjør om Tjenesten vil fungere. Signalforholdet kan forbedres vha plassering modem og/eller montering av ulike antennetyper, internt og eksternt. Dette kan først bekreftes under installasjonsfasen.

Tabell 4-1 under viser teoretiske verdier for kapasitet og indikasjon på forsinkelse som kan oppnås ved bruk av ulike teknologier for 4G Backup.

Teknologi	Data hastighet	Bandwidth	Kommunikasjons type	Forsinkelse (RTT)
3G	384 – 2048 Kbps	5-20 Mhz	Circuit switching	125-300 ms
4G	10 - 60 Mbps	100+ Mhz	Packet switching	20-50 ms

Tabell 4-1: Typiske kapasitet - og forsinkelsesverdier.

Hastighetene over er gjennomsnittlige hastigheter observert over multiple bærer nettverk på forskjellige tidspunkt av dagen. Faktiske hastigheter varierer avhengig av antall brukere, distanse til basestasjoner og signal styrke/interferens. Ved bruk av integrert ruter med SIM kort konfigureres CE-ruteren standard, slik at ruteren velger radiobånd i auto-modus. I auto-modus velger ruteren LTE(4G) dersom signalene er bedre en -100dBM, om ikke, faller ruteren tilbake på den teknologien som gir best signaler, 3G (HSDPA [UMTS+], UMTS) eller 2G (EDGE[GPRS+], GPRS).

For en stabil forbindelse kreves det at RSSI er > -90dBm. En forbindelse med RSSI = -125dBm betyr at det ikke er signal.

4.2.4 IPVPN 4G Backup - Standard vs Premium

IPVPN 4G Backup er tilgjengelig i to varianter, Standard og Premium.

Fordelen med Premium versjonen er integrert dual SIM, VPNview statistikk og roaming. Fordelen til Standard er utnyttelse av 450 Mhz båndet, dedikert mobil-modem og at den ikke avhengig av å ha mobilstøtte i CE ruter. Se tabell under.

Funksjonalitet	Standard	Premium
Produkt	4G Backup	4G Backup
Mobiloperatør/-nett	ICE.net	Nettverksuavhengig
SNMP	-	√
Roaming	-	√
VPNview2	-	√
Dedikert mobil-modem	√	-
SIM kort integrert i CE ruter	-	√

4.2.5 Diversitet

Diversitet er en tilleggstjeneste som forsikrer kunden om at to forskjellige aksesser er levert med fysisk adskillelse fra utstyr, kabler og grøfter mellom lokasjon A og lokasjon B. Dette gjelder både kunde-lokasjon og node-lokasjon i leverandørens nettverk. Tjenesten er kun tilgjengelig for Managed IPVPN.

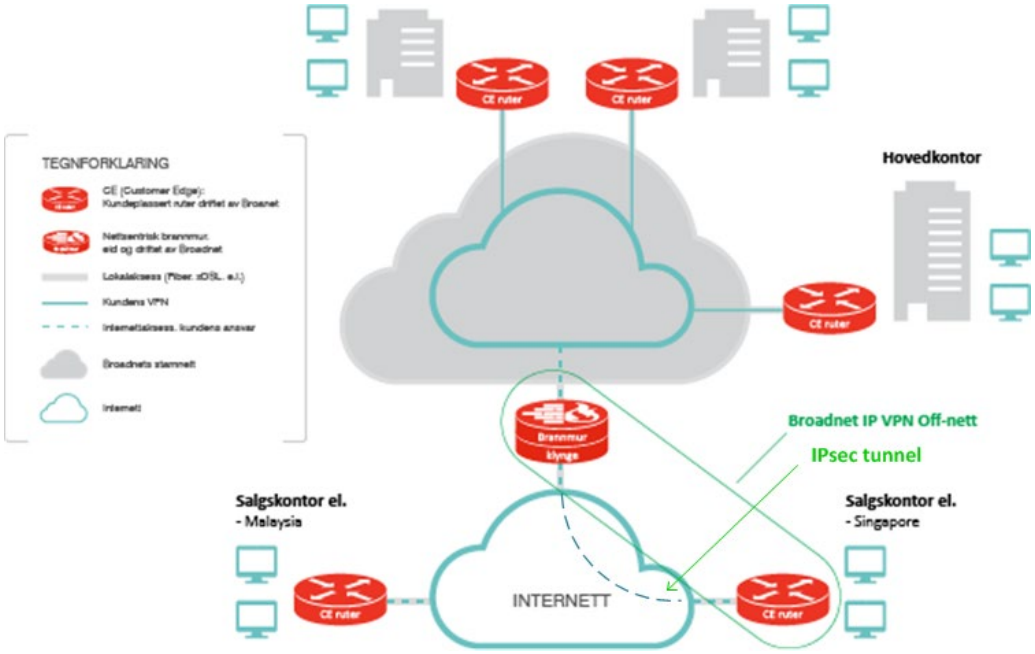
- Diversitet leveres slik at to aksesslinjer ikke har felles føringer, utstyr eller noderom
- Diversitet er alltid mellom to aksesser
- Fremføringer av et Diversitetssamband kan ikke være i samme grøft, rør, kum eller koblingsboks og det skal minst være en distanse på 5 meter i mellom
- Fremføringer kan fysisk passere hverandre, men skal da ha minimum 5 meters separasjon. For eksempel: Bakke og luft

GlobalConnect utleverer ikke detaljert informasjon om enkelt samband og deres diversitet eller nettstrukturer, uten spesiell avtale, på grunn av ekomlovens krav om skjerming verdige objekter.

4.3 IPVPN o/Internett – tilknytning av lokasjoner via Internett

Det primære dekningsområdet til IPVPN er Skandinavia; Norge, Sverige, Danmark samt Finland. Flere kunder har imidlertid en eller flere lokasjoner utenfor dette området. Disse lokasjonene kan inkluderes i kundens WAN-løsning ved å benytte tjenesten IPVPN o/Internett. IPVPN o/Internett realiseres med kryptert forbindelse over Internett. GlobalConnect vil for disse lokasjonene levere IPSec-baserte VPN som termineres nettsentrisk i GlobalConnects kjernenett via brannmur og gjøres tilgjengelig for resten av kundens IPVPN Managed-løsning. På kundelokasjonene installeres en CE-ruter som ivaretar 3DES kryptering (eventuelt DES dersom 3DES ikke tillates av lokale myndigheter) mot GlobalConnects kjernenett.

Figur 3-3 under viser en prinsippskisse av en løsning som inkluderer to IPVPN o/Internett-lokasjoner.



«Customer Edge» ruter, eid og driftet av GlobalConnect

Figur 3-3: Prinsippskisse for bruk av tjenesten IPVPN o/Internett i Malaysia og Singapore.

IPVPN o/Internett-lokasjonen kan være medlem av flere parallelle nett ved at det settes opp flere VPN-tunneler. Trafikkprioritering er imidlertid ikke tilgjengelig for IPVPN o/Internett-lokasjoner.

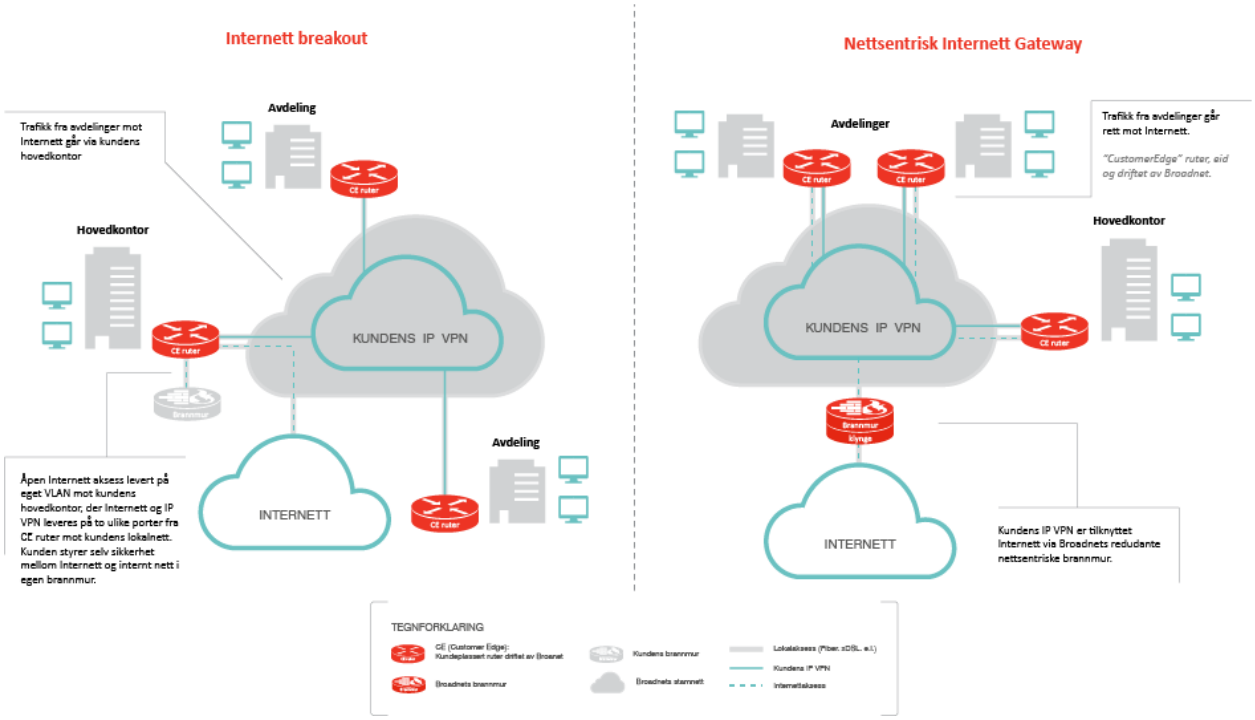
Kunden må selv skaffe til veie, eller benytte en eksisterende, internettaksess som lokalaksess mot CE-ruteren. Det forutsettes at internettaksessen har en fast, offisiell IP-adresse.

Utover ovennevnte forutsetninger legger ikke GlobalConnect noen føringer på hvilke internettleverandører (ISP) kunden benytter eller hvilken kvalitet som kreves av aksessen. GlobalConnect vil imidlertid ikke ha noe driftsansvar for internettaksessen. Dette betyr også at GlobalConnects Servicegarantier frafaller der tjenesten IPVPN o/Internett benyttes.

På tross av ovennevnte forbehold, vil bruk av IPVPN o/Internett gi kunden et helhetlig nett også utenfor Skandinavia og Finland, eller i Norge der tilgang til aksess er utfordrende.

4.4 Internettaksess i IPVPN

Internettaksess kan leveres sammen med IPVPN Managed på flere måter.



Figur 4-4: Eksempel på en IPVPN Managed basert løsning med sikret og usikret internettaksess levert nettsentrisk.

4.4.1 Internett Breakout

Internett Breakout kan konfigureres pr kunde lokasjon, men anbefales levert på et sentralt punkt i Kundens nett. Tjenesten gir direkte tilgang til Internett uten noen form for sikkerhet. Kunden ivaretar selv sikkerhet mot Internett i sin egen brannmur.

Dersom Internett Breakout leveres på en sentral lokasjon hos kunden, for eksempel på kundens hovedkontor eller datasenter, kan øvrige lokasjoner kommunisere mot Internett via kundens sentrale lokasjon. Med denne løsningen vil internettrafikk transporteres over samme lokalaksess som all annen trafikk i kundens nett. Trafikkprioritering kan imidlertid implementeres for å sikre prioritet av annen type forretningskritisk trafikk.

4.5 Nettsentrisk brannmur for IPVPN

For mange er IT-sikkerhet komplisert og distraherer virksomheten i den daglige driften. Med nettsentrisk sikkerhet tilbyr GlobalConnect sikkerhet levert som en tjeneste.

Med et uoversiktlig trusselbilde og en økning av angrep mot kritiske tjenester og infrastruktur, er det ikke nok å stole på teknologier alene. Det er essensielt å ha tilgang til kompetanse for å beskytte seg mot trusler.

I GlobalConnect er det samlet ressurser i et operasjonssenter for Nettverk og Sikkerhet (NOC/SOC) som jobber 100 % med å beskytte kunder og infrastruktur.

4.5.1 Brannmurfunksjonalitet

Tjenesten inkluderer en logisk Internettforbindelse og et sett av sikkerhetsfunksjoner og består av:

- Logisk forbindelse til Internett som leveres i hastighets-steg fra 2 Mbps til 1 Gbps
- For IPVPN finnes 3 definerte funksjonalitetspakker(Standard, Plus og Premium)
- Enkelte tjenester bestilles som en opsjon og er merket <Opsjon> i tabellen under.

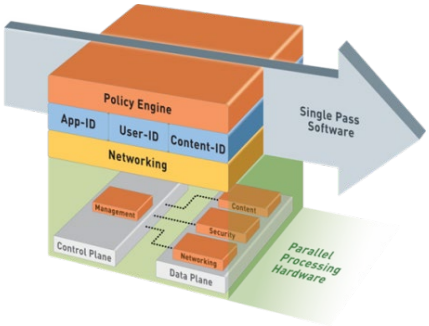
TJENESTE	STANDARD	PLUS	PREMIUM	BESKRIVELSE
Applikasjonsbruk	√	√	√	Ser applikasjonsbruken i nettverket. Mulig å sette alarmnivå for brudd på policy
Applikasjonskontroll	√	√	√	Blokkere uautorisert Internettrafikk basert på applikasjonstype.
Standardrapport	√	√	√	Regelmessig rapportering på nettverkstrafikk
Anti-virus og Anti-Spyware	X	√	√	Beskyttelse mot ondsinnet trussel som kan medføre tap av data og nedetid.
URL-filtrering	X	√	√	Unngå uønsket innhold. Reduserer risiko for brudd på juridiske og regulatoriske forhold. Økt produktivitet.
Tilpasset sikkerhetspolicy	X	√	√	Tilpasser sikkerheten i henhold til bedriftens sikkerhetspolicy. Kan tilpasses individuelle brukere, grupper eller lokasjoner. Krever integrasjon med AD
Tilpasset rapport	X	√	√	Tilpasset rapport med informasjon til ulike interessenter.
Forebygge inntrenging (IPS)	X	X	√	Beskyttelse mot uautorisert og ondsinnet tilgang som kan resultere i tap av data og nedetid
Fil-filtrering	X	X	√	Reduserer risikoen for uautorisert filoverføringer inn og ut av bedriftens nettverk.
Sikker fjernaksess	X	Opsjon	Opsjon	Gir brukere utenfor kontoret sikker tilgang til ressurser i bedriftens intern-nett.
Sikker kommunikasjon mellom lokasjoner	X	Opsjon	Opsjon	Sikker kryptert kommunikasjon mellom ekstern lokasjon og bedriftens VPN
Brukeridentifikasjon	X	Opsjon	Opsjon	Retningslinjer definert i katalogtjeneste (f.eks. Active Directory) kan synkronisere regelsett/policy definert i brannmuren.
Sikkerhetssone	X	Opsjon	Opsjon	Separate soner, f.eks Demilitær sone (DMZ), gjestenett etc.

√ = Inkludert X = Ikke tilgjengelig

Brannmurtjenesten identifiserer applikasjoner, innhold og trusler og trafikken i samsvar med kundes sikkerhetspolicy. Brukere får tilgang til ønsket informasjon og sikres mot trusler fra Internett.

Kort oppsummert vil tjenesten:

- Identifisere applikasjoner (App-ID)
- Identifisere brukere (User-ID)
- Sjekke innholdet (Content-ID)



4.6 Betalingsaksess

4.6.1 NETS tilgang

Tilgang til betalingsaksess løses via en nettsentrisk brannmur lokalisert i GlobalConnects kjernenett, for å gi sikker tilgang.

Nettsentrisk betalingsaksess passer for kunder med integrerte backoffice/terminalkasser og/eller kunder med et relativt stort antall lokasjoner som kjører betalingstransaksjoner. Løsningen baserer seg på dedikert VPN, også kalt Service VPN, kun for terminal/betalings-transaksjons trafikk.

Samtlige lokasjoner kan kommunisere mot betalingsleverandøren uten å gå om kundens hovedkontor eller datasenter, samtidig som sikkerheten ivaretas i brannmuren.

Aksesskapasiteten per lokasjon utnyttes optimalt ved å kombinere intranett-trafikk og betalings-transaksjoner på samme aksess. Trafikkprioritering kan implementeres for å sikre prioritering av forretningskritiske applikasjoner. Løsningen følger IPVPN Managed design og gir samme redundansnivå som er bygget inn i denne.

5 Service Level Agreement - SLA

Som del av IPVPN Managed tjenesten inngår en definert tjenestekvalitet – også kalt Service Level Agreement (SLA). SLA-et spesifiser hvilken kvalitet som er avtalt mellom kunden og GlobalConnect for tjenesten IPVPN Managed.

GlobalConnects Service Level Agreement (SLA) for IPVPN Managed er bygget opp slik at kvalitetsnivået på tjenesten kan tilpasses kundens behov og/eller kost/nytte analyse per lokasjon. Dette, sammen med de tilgjengelige rapporteringsmuligheter, gir kunden et forutsigbart nett og gode muligheter for oppfølging av løsningens kvalitetsnivå.

Hver kvalitetsparameter har et forhåndsdefinert kvalitetsnivå som angir om tjenesten IPVPN Managed ligger innenfor avtalt kvalitet. Kvalitet i GlobalConnects MPLS-nett er bestemt av kriteriene angitt her. Tjenesten leveres med en avtalt Servicetid og en avtalt Servicegaranti. Aksessforbindelser som GlobalConnect leier av andre leverandører mellom Stamnett og Kundens lokaler, kan avvike fra disse krav og kriterier.

Vær oppmerksom på at det per i dag kan finnes variasjoner i avtalt kvalitetsnivå for kundelokasjoner utenfor Norge. For disse lokasjonene vil teknisk personell hos GlobalConnect, på forespørsel, vurdere hvilket avtalt kvalitetsnivå GlobalConnect kan tilby per kvalitetsparameter basert på lokasjonens beliggenhet og krav.

5.1 Servicetid

Servicetiden spesifiserer det tidsrommet som GlobalConnect utfører feilretting på tjenesten. Kunden kan velge Basis, Utvidet eller Kontinuerlig Servicetid. Dersom det ønskes feilretting ut over det som er avtalt Servicetid må dette bestilles i hvert enkelt tilfelle med en tilhørende kostnad for utrykning og arbeid. GlobalConnect kan ikke garantere at slik feilretting kan utføres.

5.2 Servicegaranti

GlobalConnects redundante stamnett er konstruert for høy Tjenestetilgjengelighet.

Følgende Servicegarantier kan velges for tjenesten:

PARAMETER	SERVICEGARANTI 1	SERVICEGARANTI 2	SERVICEGARANTI 3
Tjenestetilgjengelighet per kvartal	99,75%	99,90%	99,99%
Fysisk feilretting (normal	< 8 timer	< 5 timer	< 3 timer
Term.feilretting (normal feilrettingstid)	< 4 timer	< 1 timer	< 3 minutter
Aksess realisering / Redundans	Enkel	Redundans/Backup	Redundans/Diversitet
Responstid	Umiddelbart	Umiddelbart	Umiddelbart
Tilbakemelding under feilretting	< 2 timer	< 30 minutter	< 10 minutter
Feilmottak	24/7/365	24/7/365	24/7/365

Tabell 5-1: Kvalitetsnivå.

5.3 Teknisk krav til Tilgjengelighet

TILGJENGELIGHET, %	SERVICEGARANTI	TEKNISK LØSNING
99.99%	Servicegaranti 3	Linjeredundans med diversitet; to CE-rutere med to redundante Fiber, Ethernet, Mobil Premium aksesser knyttet opp til to ulike PE-noder. xDSL kan ikke benyttes i en slik løsning
99.90%	Servicegararnti 2	Alternativ 1 : Fiber eller xDSL primær og 4G Backup; en CE-ruter Alternativ 2 : Fiber eller xDSL primær og 4G Backup eller xDSL; to CE-rutere, en med fiber/xDSL grensesnitt og en med fiber/xDSL/SIM kort. Sekundær xDSL skal være tilknyttet altenrativ PE node
99.75%	Servicegararnti 1	Managed IPVPN - En CE ruter, en Aksess knyttet til en PE node
99,75%	Servicegararnti 1	Unmanaged IPVPN

6 Performance Management

6.1 Bakgrunn

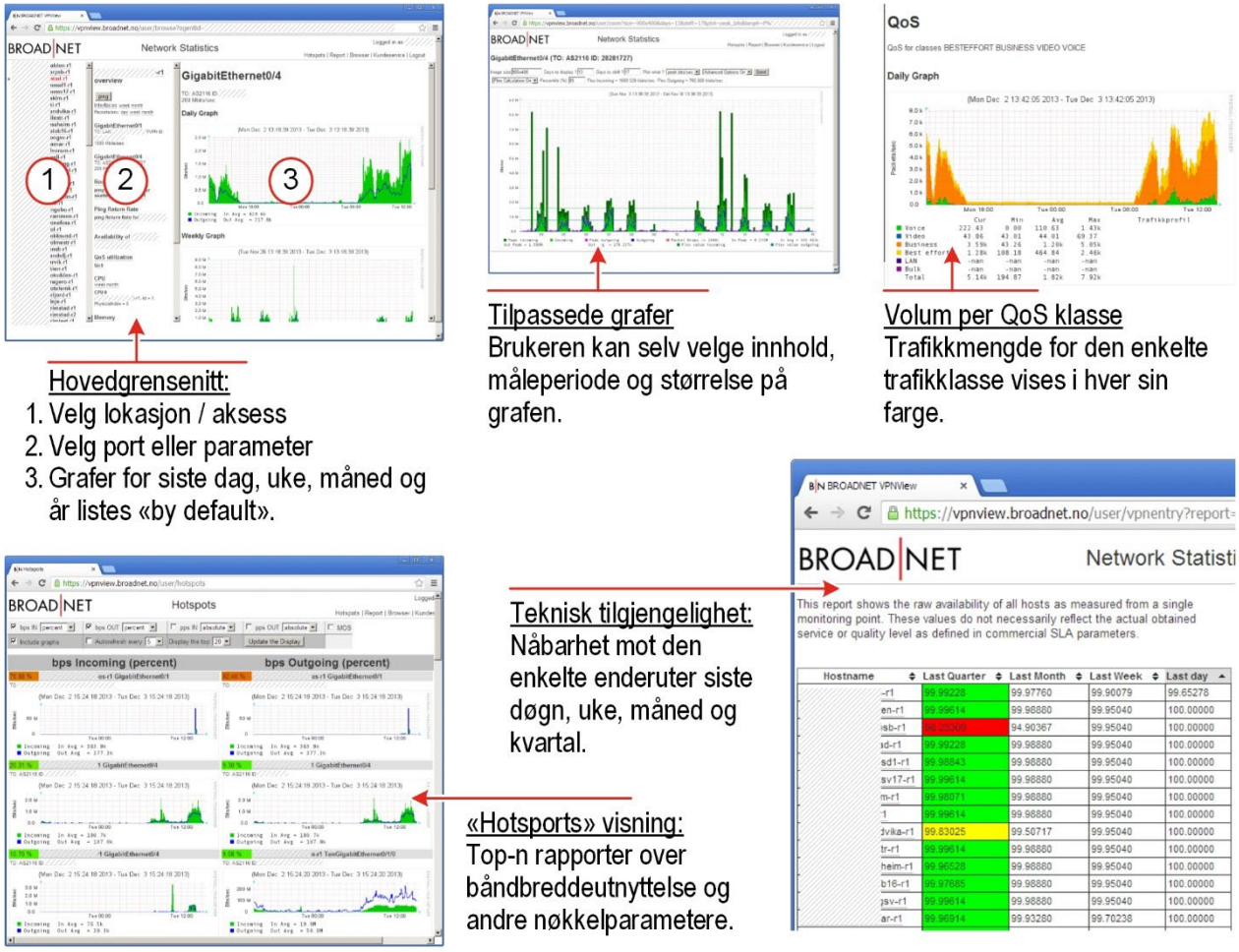
I dag, mer enn noen gang, er kundens nettverk en viktig bidragsyter for bedriftens resultater. Alle organisasjoner er avhengige av en kostnadseffektiv IT-infrastruktur for å være konkurransedyktige og vokse. Ettersom nettverket blir mer kritisk; blir det også mer komplekst i – omfang, geografisk rekkevidde, antall applikasjoner, teknologier og aksessmetoder det må støtte.

GlobalConnects løsning for "Performance Management" i kombinasjon med hensiktsmessig trafikkprioritering i nettet, vil sikre kundens kommunikasjonsløsning.

6.1.1 Performance monitoring - VPNview

Kunden vil ha web-tilgang til en egen versjon av Performance Monitoring systemet på vpnview.GlobalConnect.no.

Figur2-1 under viser et utvalg av funksjonalitet tilgjengelig i det web baserte monitoreringssystemet.



Figur2-1 - VPNview - Tilbyders Performance Monitoring system. Skjermbildene over viser et utvalg av funksjonalitet som er tilgjengelig i systemet. Øvrig funksjonalitet er beskrevet videre i dette avsnittet.

Oppsummert vil systemet gi følgende funksjonalitet for kunden:

- Hovedsiden “Dashboard” viser antall CE rutere i nettet og et oversiktsbilde av kundens nettverk. I ett bilde har kunden 4 top-N tabeller som viser Trafikk på WAN interface, Tilgjengelighet, Pakketap og Forsinkelse. Tabellene kan vises for time, uke, dag, måned, kvartal og år.
- Grafisk fremstilling av båndbreddeforbruk ved den enkelte lokasjon, fordelt på fysisk interface, nett (f.eks. gjestenett eller internt nett) eller *kvalitetsklasse*. Et eksempel på sistnevnte er vist øverst til høyre i Figur2-12-1 og vil være tilgjengelig så snart konfigurasjon av trafikkprioritering i enderuterne er oppdatert for å støtte dette.

- Ved valg av ønskede data, vil grafer for siste døgn, uke, måned og år vises. Kunden kan imidlertid tilpasse disse grafene ytterligere etter eget ønske, både med hensyn til måleperiode, størrelse på grafen og for flere av dataene, også hvilke data som skal vises. (For trafikk over fysiske porter eller VPN, kan Kunden eksempelvis velge peak bits per sekund, pakker per sekund, bytes per pakke eller feil/pakkedropp i tillegg til standardvisning for bits per sekund).

- Pakketap og forsinkelse per kvalitetsklasse samt jitter og MOS (Mean Opinion Score) for taletrafikk. Her kan Kunden i sanntid verifisere om trafikkvalitet mot den enkelte lokasjon og for den enkelte kvalitetsklasse er i henhold til avtalte verdier. MOS verdien for taletrafikk er en måleverdi for opplevd talekvalitet i IP telefoniløsninger, og kan således benyttes for å vurdere i hvilken grad kvalitet i nettet påvirker kvalitet i IP telefoni som transporteres over nettet. Som for båndbreddegrafer, vises også ovennevnte grafer i utgangspunktet for siste døgn, uke, måned og år, med mulighet for å tilpasse både måleperiode og størrelse på grafen.

- I en «Hotspots» visning, vist nede til venstre i Figur2-1, kan Kunden hente ut «topp-n» rapporter over parametere i nettet, som f.eks. de 5 lokasjonene med høyest prosentvis båndbreddeutnyttelse. Kunden velger selv antall lokasjoner som skal listes, hvilke parametere det ønskes rapport på og om det ønskes en liste med grafer eller kun numeriske verdier.

- En oversikt over teknisk tilgjengelighet, vist nede til høyre i Figur2-1, kan Kunden se teknisk tilgjengelighet for det enkelte samband i IPVPN løsningen. Her vises total nåbarhet over hvert samband, både primær- og backupsamband ved redundante lokasjoner, uansett årsak til nedetid. Dette kan altså ikke direkte relateres til avtalte oppetidsgarantier slik rapportene er beskrevet i avsnitt 5.2 kan, men viser til gjengjeld tilgjengelighet i sanntid og «ufiltrert» slik at all nedetid uansett årsak er synlig.

- Mobile Interface gir tilgang til informasjon på bånd, trafikkvolum, signalstyrke og signalkvalitet

- En «Ping» knapp i web grensesnittet for den enkelte lokasjon, gjør Kunden i stand til å verifisere om det er kontakt over det enkelte samband «akkurat nå».

Kunden har gjennom VPNview systemet tilgang til trafikkdata både for IPVPN nettet og sentral Internett aksess.

7 Priser

7.1 Prisstruktur

Prisene for tjenesten oppgis med etableringspris og en månedlig pris. Etableringsprisen for tjenesten avhenger av avtale lengde. I tillegg tilkommer priser for bl.a. internkabling, flytting og annet arbeid som ikke er inkludert i etableringsprisen.

Det kan oppnås rabatter ved å binde Tjenesten for en avtaleperiode for 2, 3, eller 5 år. Korteste avtaleperiode for Tjenesten er 12 måneder. Avtaleperioden regnes fra Faktisk Leveringsdato for hver enkelt linje som leveres.

8 Prosedyre for Feilretting og feilrettingstid

GlobalConnect overvåker Tjenesten døgnet rundt og hele året. GlobalConnects driftssenter vil oppdage mange typer feil, og vil da varsle Kunden om dette innenfor Servicetiden kunden har avtalt. I de tilfeller Kunden oppdager feil på tjenesten som ikke Kunden har fått melding om, må dette varsles til GlobalConnect så raskt som mulig. Før Kunden melder feil til GlobalConnect er det viktig at eget Utstyr sjekkes. Hvis en kundemeldt feil viser seg å ligge i Kundens Utstyr, vil GlobalConnect ta betalt for feilsøkingen.

Dersom det oppstår en feil eller et problem, skal de nødvendige undersøkelser og feilrettingstiltak påbegynnes i henhold til GlobalConnects spesifikasjoner for feilhåndtering. Feil kan rapporteres pr. telefon, eller e-post. GlobalConnects Kundeservice behøver følgende opplysninger:

- Sambandsnummer
- Beskrivelse av feilen
- Modem status (hvis mulig) og bekreftelse på at eget Utstyr er sjekket
- Telefonnummer, telefaks nummer og e-postadresse til kontaktperson hos Kunden for test og adgang
- Tidspunkt for når feilen ble oppdaget
- Berørt adresse (der det er aktuelt)
- Eventuelle andre relevante opplysninger

Feilrapporter og bekreftelser blir rapportert til Kunden pr. telefon eller e-post etter godkjent prosedyre.

Aksesser som er realisert som ADSL eller SHDSL-aksesser har som standard ingen garantier for feilrettingstid. Mot et tillegg i prisen er det mulig å bestille oppgradering med en garanti for feilrettingstid for aksessen.

Vedlegg A - Standard klassifiseringsoppsett QoS

Dersom kunden ønsker det kan GlobalConnect klassifisere trafikken iht. et standard oppsett, slik det er spesifisert i Tabell 8-1 nedenfor.

Det er trafikk i Businessklassen som merkes ved bruk av standardoppsettet.

APPLIKASJON	TRANSPORT	PORT NR	PORT RANGE
Citrix	TCP/UDP	1494, 1604, 2598	
SAP	TCP/UDP		3200 3399
RDP Remote Desktop Protocol	TCP	3389	
TELNET	TCP	23	
SQL	TCP	1433	
DISPLAY SYSTEMS PROTOCOL	TCP/UDP	246	

Tabell 8-1: GlobalConnect klassifisert trafikk, standard oppsett for prioritering i Businessklassen.

Vedlegg B - Forkortelser og definisjoner

Forkortelse/Definisjon	Forklaring
IPVPN-aksess	IPVPN-aksess Består av komponentene lokalaksess og VPN-forbindelsen gjennom GlobalConnects kjernenett.
3DES	Triple Data Encryption Standard Krypteringsalgoritme for sikker kryptering av data. Videreutvikling av DES, som i enkelte land fortsatt er eneste tillatte krypteringsalgoritme
ADSL	Asymmetric Digital Subscriber Line En eksisterende telefonlinje hos kunden benyttes for transport av data mot leverandørens nett. I Norge benytter alle ADSL leverandørene telefonlinjene som opprinnelig ble etablert av det som i dag er Telenor. Hos kunden termineres ADSL-aksessen i et modem eller en ruter/switch. I telefonsentralen knyttes aksessen mot den aktuelle ADSL-leverandørens utstyr. ADSL er asymmetrisk, som betyr at kunden får større båndbredde inn (nedlastning) enn ut (opplastning).
Aksess el. lokalaksess	Aksess el. lokalaksess Forbindelse som knytter kundens lokasjon til GlobalConnects kjernenett – fra modem til PE-ruter.
Alternativ infrastruktur	Alternativ Infrastruktur Infrastruktur for leveranse av aksesser der GlobalConnect ikke kan levere på egen infrastruktur. Aksess fra tredjepart operatør.
BBS	Bankenes Betalings Sentral Se Nets.
CE-ruter/switch	Customer Edge ruter/switch Ruter/switch plassert på kundelokasjon, kan enten være driftet av GlobalConnect, forhandler/tjenesteleverandør eller kunden selv.
DHCP	Dynamic Host Configuration Protocol Automatisk tildeling av IP-adresse og annen IP-konfigurasjon til PC-er og andre nettverksenheter.
DSL	Digital Subscriber Line Fellesbetegnelse for ADSL og SDSL/SHDSL. Se definisjon av ADSL, SDSL og SHDSL for ytterligere beskrivelse.
Ferdigmelding	Ferdigmelding Ferdigmelding sendes til kunden etter at bestilt tjeneste/endring er levert og inneholder dato for start av fakturering av tjenesten.
Ferdigsjekk	Ferdigsjekk GlobalConnects leveransekontroll for å sikre at tjenesten er levert iht. beskrevet funksjonalitet.
HSRP	Hot Standby Router Protocol

Forkortelse/Definisjon	Forklaring
	Teknologi som gjør at en sekundær ruter (”hot standby router”) automatisk overtar IP-adressen til den primære ruteren dersom denne ruteren mister kontakt med nettet eller selv blir utilgjengelig.
Informasjonsmelding	Informasjonsmelding Melding om eventuelle avvik i leveranseprosessen som måtte avdekkes. Inneholder en beskrivelse av avviket og informasjon om mulige tiltak.
IP	Internet Protocol Nettverksprotokoll utviklet for det som i dag er Internett (derav navnet), men er i dag den mest brukte protokollen for rutede nett.
IPVPN	IP Virtual Private Network IP-basert Virtuelt Privat Nettverk. Fellesbetegnelse for flere teknologier benyttet for WAN – geografisk utbredte nettverk. Nettene implementeres som virtuelle separate nett over tjenesteleverandørens felles nettverk, og er basert på transport av IP.
ISP	Internet Service Provider Selskap som selger og leverer internettjenester.
Jitter	Jitter Variasjon i forsinkelse mellom et gitt punkt A til et gitt punkt B.
Kunde	Kunde Kontrakts holder mot GlobalConnect og/eller kunde av forhandler eller videreselger som forhandler IPVPN-tjenestene.
Kvalitetsparameter	Kvalitetsparameter Benevnelse på de ulike parameterne man måler kvalitet mot i avtalt Service Level Agreement/tjenestekvalitet for IPVPN. Eksempler på kvalitetsparametere er; tilgjengelighet, jitter, RTD og normal rettetid.
LAN	Lokal Area Network Ofte omtalt som lokalnett. Et LAN er et nett som binder sammen enheter innenfor et geografisk begrenset område, gjerne innenfor en og samme bygning. Man omtaler ofte flere separate lokalnett der det er begrensninger i kommunikasjon mellom nettene som separate LAN.
Leveringsdato	Leveringsdato Den dagen en bestilt tjeneste/endring er tilgjengelig for bruk av kunden.
Leveringstid	Leveringstid Tiden fra GlobalConnect mottar korrekt bestilling og frem til leveringsdato.
LTE	Long-Term Evolution. Ofte markedsført som 4G og er en standard for trådløs kommunikasjon av data i høy hastighet for mobiltelefoner og dataterminaler.
MPLS	Multi Protocol Label Switching

Forkortelse/Definisjon	Forklaring
	Nettverksprotokoll som tillater transport av flere separate nett over samme linjer og nettverkskomponenter. Separasjonen kan sammenlignes med VLAN, men MPLS gir blant annet bedre mulighet for å rute trafikken over redundante føringsveier. GlobalConnect benytter MPLS i sitt kjernenett for å kombinere separasjon av de enkelte kundene sine nett og samtidig ivareta redundans.
Nets	Nets Selskap som håndterer elektronisk IS og betalingstransaksjoner. Tidligere BBS (Norge) og PBS (Danmark).
NTP	Nett Termineringspunkt Termineringspunkt for aksesslinjen.
Pakketap	Pakketap En prosentandel av pakker fra et gitt punkt A som ikke når frem til et gitt punkt B.
PE-ruter	Provider Edge ruter Ruter i GlobalConnects MPLS-baserte kjernenett for tilkopling av kundelokasjoner.
QoS	Quality of Service Definisjonen brukes ofte i flere sammenhenger. I forbindelse med IPVPN er det kvaliteten definert for tjenesten og/eller brukeren opplever, ev. per trafikkklasse, som omtales som QoS.
RTD	Round Trip Delay Den tiden det tar trafikk å nå fra et gitt punkt A til et gitt punkt B og tilbake igjen. Dette er eksempelvis verdien som presenteres som ”round trip delay” når man kjører kommandoen ping fra en lokasjon til en annen.
SDSL	Symmetric Digital Subscriber Line En eksisterende telefonlinje hos kunden benyttes for transport av data mot leverandørens nett. I Norge benytter alle SDSL-leverandørene telefonlinjene som opprinnelig ble etablert av det som i dag er Telenor. Hos kunden termineres SDSL-aksessen i et modem eller en ruter/switch. I telefonsentralen knyttes aksessen mot den aktuelle SDSL-leverandørens utstyr. SDSL er, i motsetning til ADSL, symmetrisk, som betyr at kunden får samme båndbredde inn (nedlastning) som ut (opplastning).
SHDSL	Symmetric High-Speed Digital Subscriber Line Overordnet er SHDSL det samme som SDSL. I forbindelse med IPVPN er det begrepet SHDSL som benyttes. Se også SDSL.
SLA	Service Level Agreement Avtale mellom GlobalConnect og kunde om tjenestenivå. Betegnes også ”tjenestekvalitet”.

Forkortelse/Definisjon	Forklaring
SNMP	Simple Network Management Protocol Protokoll for innhenting av teknisk driftsinformasjon fra enheter i nettverket.
Tjenestekvalitet	Tjenestekvalitet Avtale mellom GlobalConnect og kunden om tjenestens kvalitetsnivå. Betegnes også som ”SLA”.
Trafikklasser	Trafikklasser Tjenesteklasser med ulik definert kvalitet tilpasset ulike applikasjoners karakteristikk og for prioritering av disse.
Tredjepart operatør	Tredjepart operatør Operatør som leverer alternativ aksess der GlobalConnect ikke kan levere på egeneid infrastruktur.
GlobalConnect kjernenett	GlobalConnect kjernenett GlobalConnects MPLS-baserte stamnett. Skandinavisk dekning.
Virkedag	Virkedag Arbeidsdag mandag - fredag, unntatt helligdager.
VDSL	Very-high-bit-rate digital subscriber line Asynkron DSL aksess på lik linje som ADSL, men med høyere hastigheter. Se for øvrig pkt ADSL.
VLAN	Virtual LAN (Local Area Network) Flere LAN (se egen forklaring) transporteres over samme linjer, kabler eller svitsjer uten mulighet for å kommunisere internt.
VPN	Virtual Private Network Betegnes på norsk for ”virtuelt privat datanett”. Er betegnelsen på en datateknikk som anvendes for å skape ”punkt-til-punkt”-forbindelser, såkalte «tunneler», gjennom et annet datanett som eksempelvis Internett eller operatørers private nett. Man kan ha krypterte VPN eksempelvis basert på IPSec, SSL eller L2TP eller såkalte ”trusted VPN” som eksempelvis kan basere seg på MPLS (Multi Protocol Label Switching).
VRF	Virtual Routing and Forwarding Muliggjør flere separate rutingtabeller på en og samme ruter. Dette gjør blant annet at man i praksis kan benytte en og samme ruter til å transportere flere nett som ikke skal kommunisere seg imellom.
WAN	Wide Area Network Et nett som binder sammen enheter innenfor et spredt geografisk område.